Configurazione di SWA Second Factor Authentication con ISE come server RADIUS

Sommario

Introduzione

In questo documento viene descritto come configurare l'autenticazione di secondo fattore su Secure Web Appliance con Cisco Identity Service Engine come server RADIUS.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze di base in SWA.
- Conoscenza della configurazione dei criteri di autenticazione e autorizzazione su ISE.
- Conoscenze base di RADIUS.

Cisco consiglia inoltre di:

- Accesso amministrativo per Secure Web Appliance (SWA) e Cisco Identity Service Engine (ISE).
- L'ISE è integrata in Active Directory o LDAP.
- Active Directory o LDAP è configurato con un nome utente 'admin' per autenticare l'account 'admin' predefinito SWA.
- Versioni compatibili WSA e ISE.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- SWA 14.0.2-012
- ISE 3.0.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Quando si abilita l'autenticazione di secondo fattore per gli utenti amministrativi su SWA, il dispositivo verifica le credenziali utente con il server RADIUS per la seconda volta dopo aver verificato le credenziali configurate in SWA.

Topologia della rete

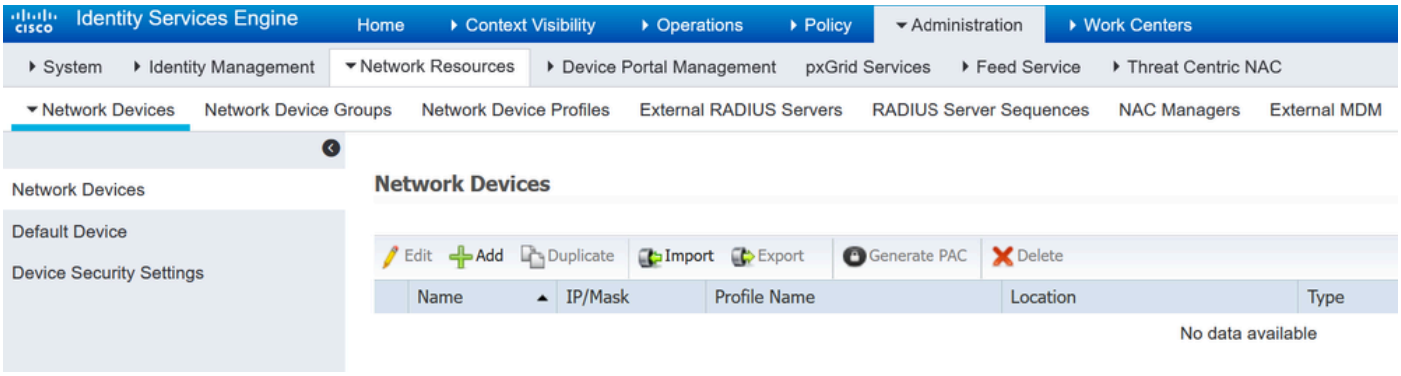
Immagine - Diagramma della topologia di rete

Gli utenti con privilegi amministrativi accedono all'interfaccia SWA sulla porta 443 con le proprie credenziali. SWA verifica le credenziali con il server RADIUS per l'autenticazione del secondo fattore.

Procedura di configurazione

Configurazione di ISE

Passaggio 1. Aggiungere un nuovo dispositivo di rete. Selezionare Amministrazione > Risorse di rete > Dispositivi di rete > +Aggiungi.



Aggiungi SWA come dispositivo di rete in ISE

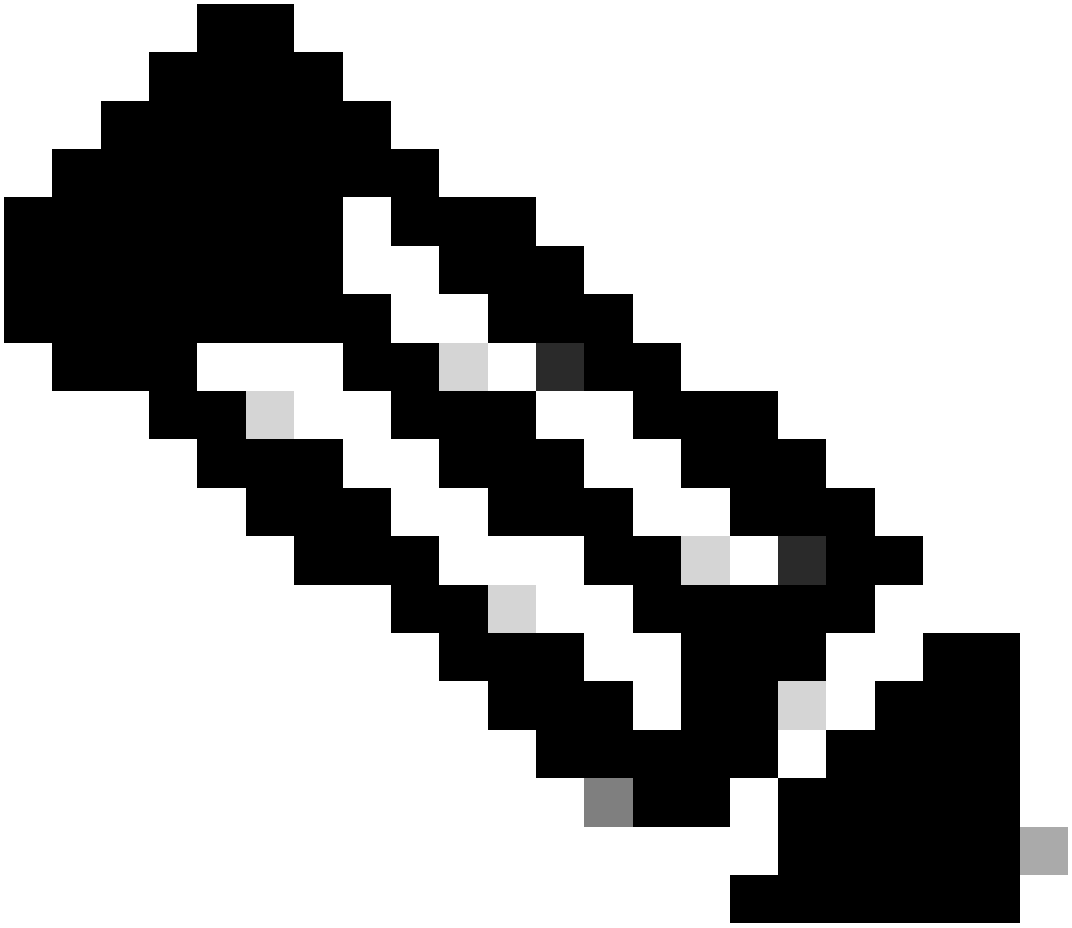
Passaggio 2. Configurare il dispositivo di rete in ISE.

Passaggio 2.1. Assegnare un Name all'oggetto dispositivo di rete.

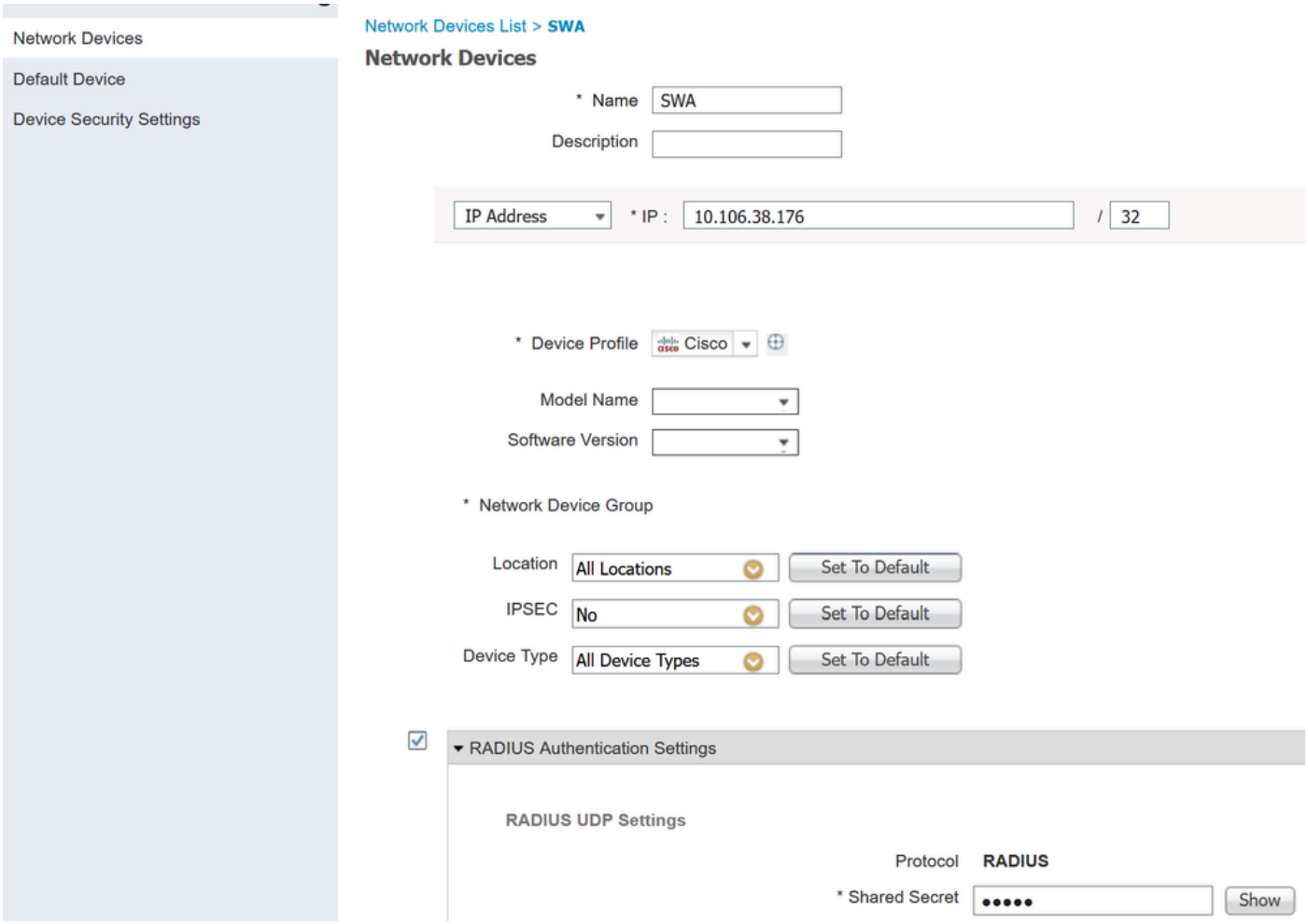
Passaggio 2.2. Inserire l'indirizzo IP SWA.

Passaggio 2.3. Selezionare la casella di controllo RADIUS.

Passaggio 2.4. Definire un segreto condiviso.

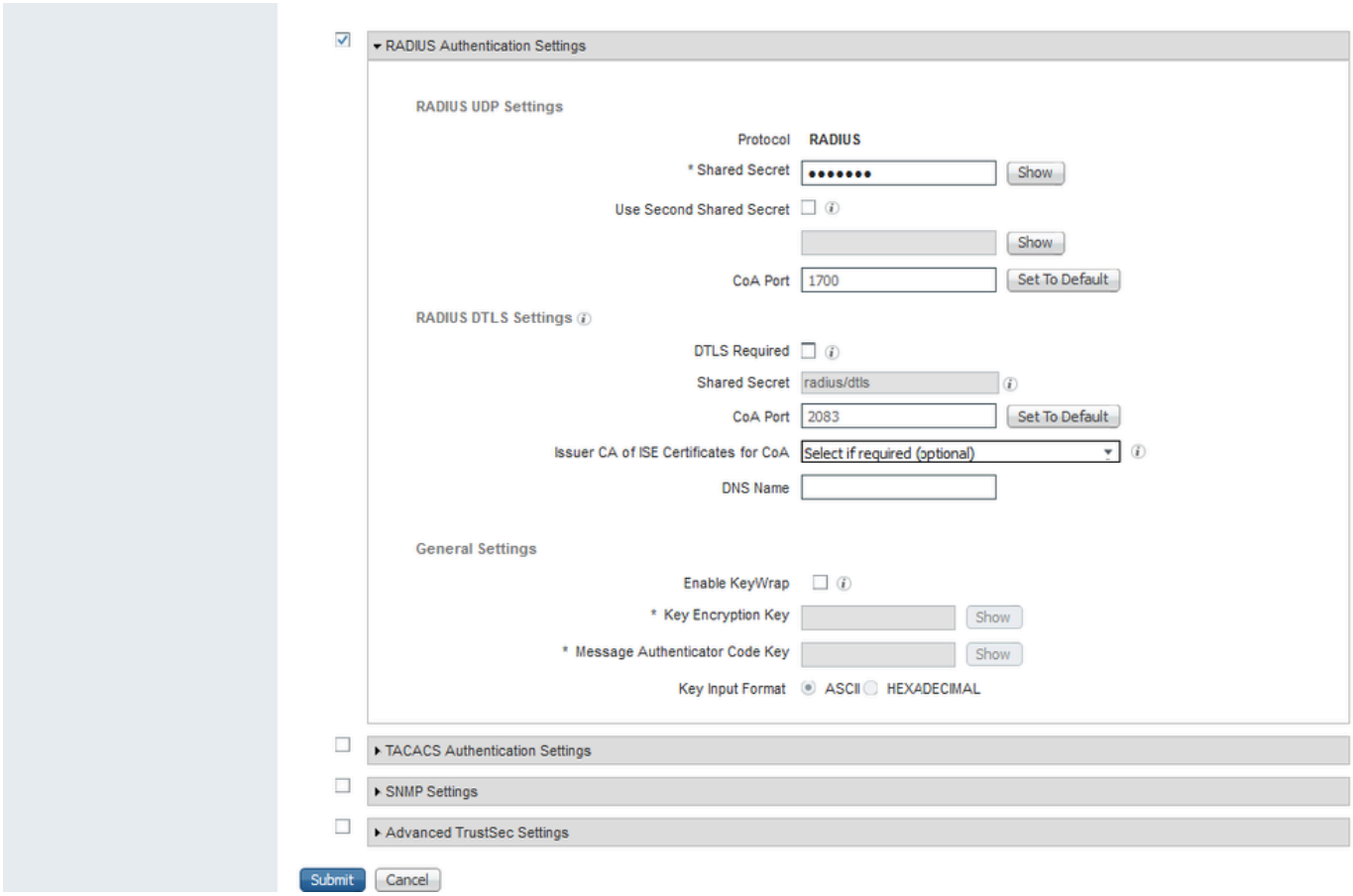


Nota: la stessa chiave deve essere utilizzata successivamente per configurare l'SWA.



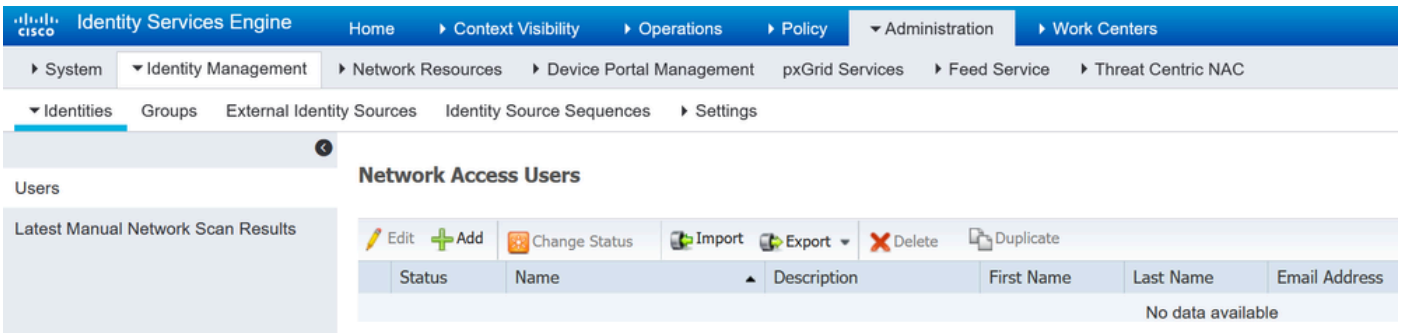
Configurazione della chiave condivisa del dispositivo di rete SWA

Passaggio 2.5. Fare clic su Invia.



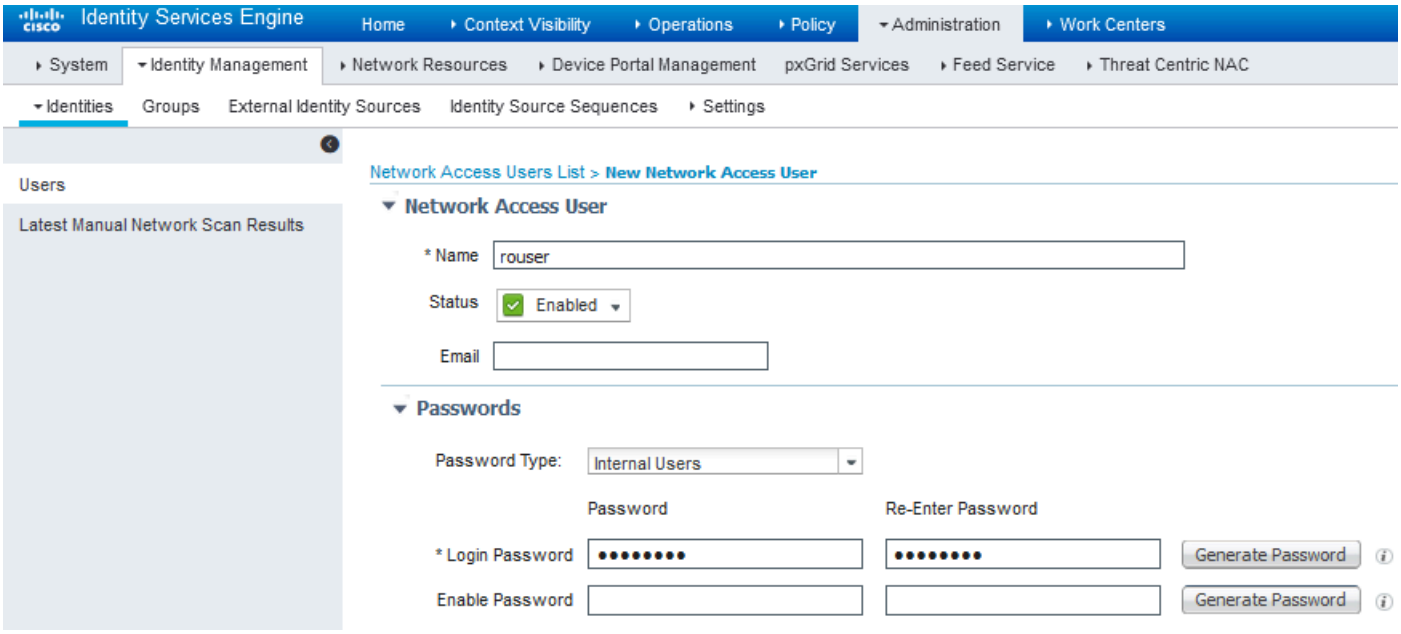
Invia configurazione dispositivo di rete

Passaggio 3. È necessario creare utenti di accesso alla rete corrispondenti al nome utente configurato in SWA. Passare a Amministrazione > Gestione delle identità > Identità > + Aggiungi.



Aggiungi utenti locali in ISE

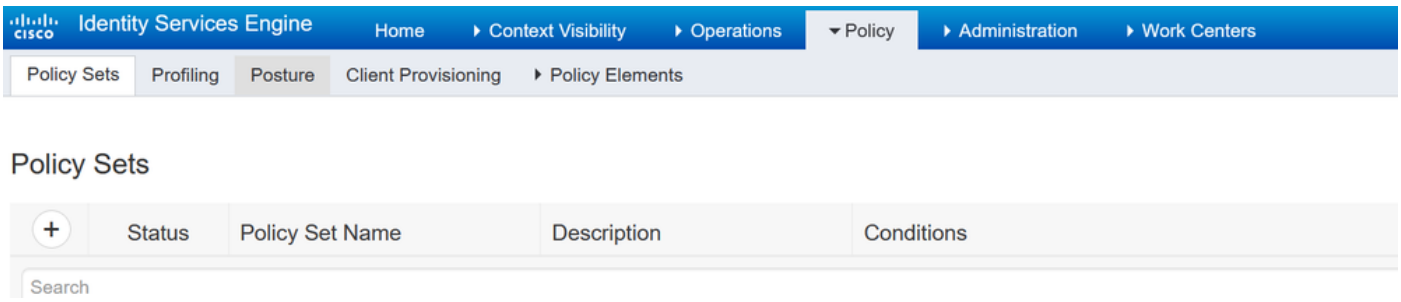
Passaggio 3.1. Assegnare un nome.
Passaggio 3.2. (Facoltativo) Immettere l'indirizzo e-mail dell'utente.
Passaggio 3.3. Imposta password.
Passaggio 3.4. Fare clic su Save (Salva).



Aggiungere un utente locale ad ISE

Passaggio 4. Creare un set di criteri corrispondente all'indirizzo IP SWA. In questo modo è possibile impedire l'accesso ad altre periferiche con queste credenziali utente.

Passare a Policy > PolicySets e fare clic sull'icona + posizionata nell'angolo superiore sinistro.

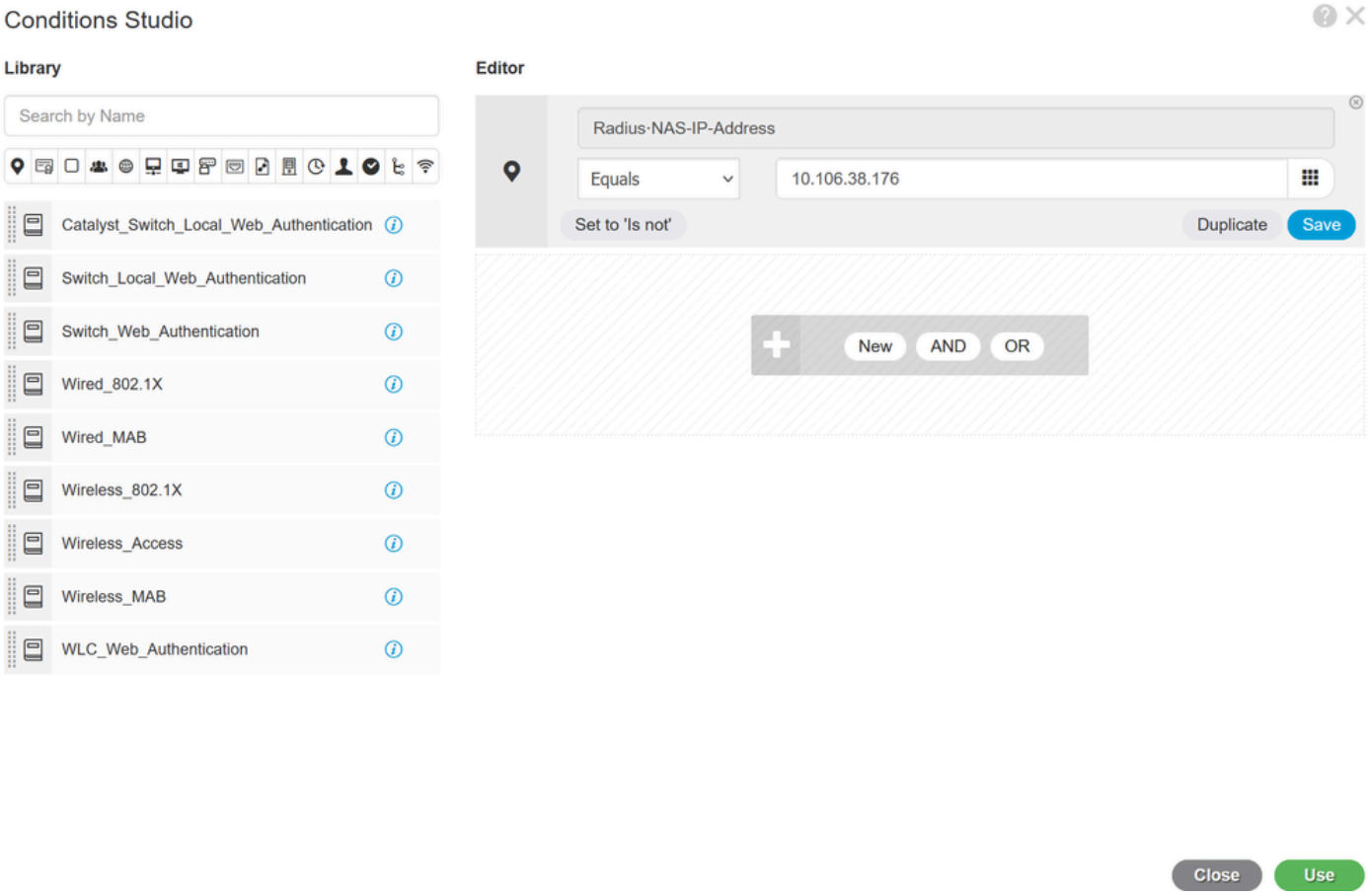


Aggiungi set di criteri in ISE

Passaggio 4.1. Nella parte superiore dei set di criteri viene inserita una nuova riga. Immettere il nome per il nuovo criterio.

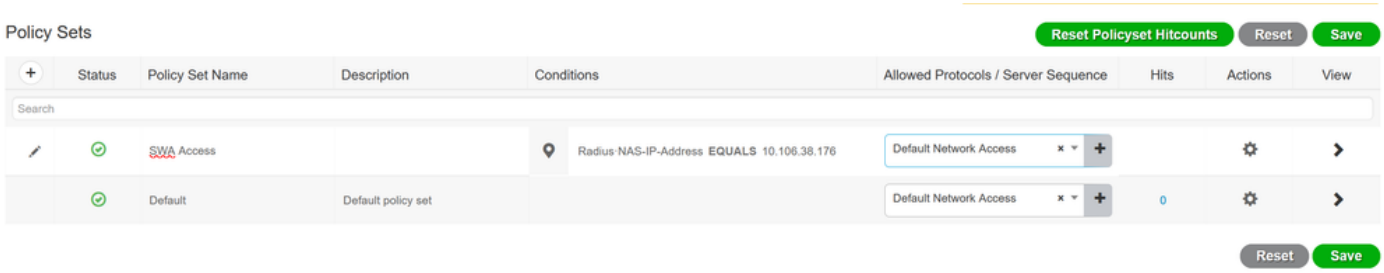
Passaggio 4.2. Aggiungere una condizione affinché l'attributo RADIUS NAS-IP-Address corrisponda all'indirizzo IP SWA.

Passaggio 4.3. Fate clic su Usa (Use) per mantenere le modifiche e uscire dall'editor.

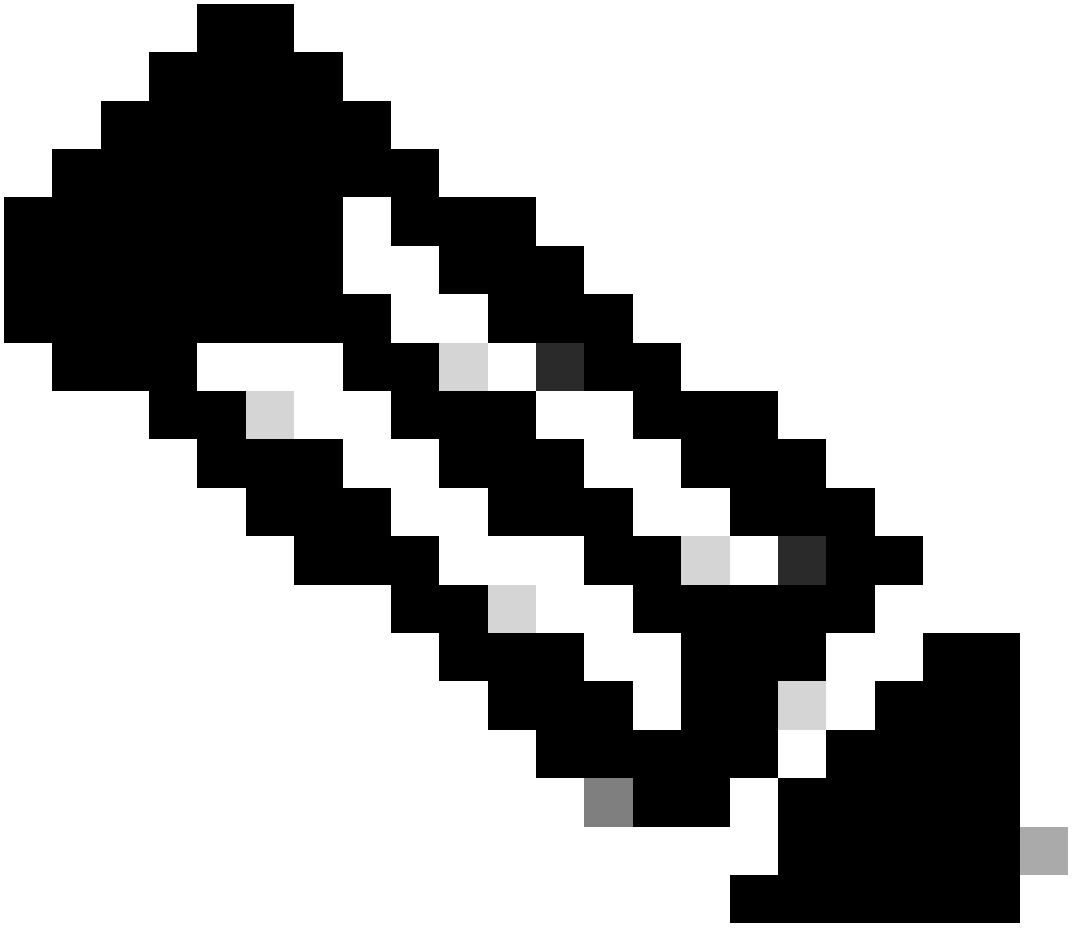


Aggiungi criterio per mappare il dispositivo di rete SWA

Passaggio 4.4. Fare clic su Save (Salva).



Salvataggio criteri



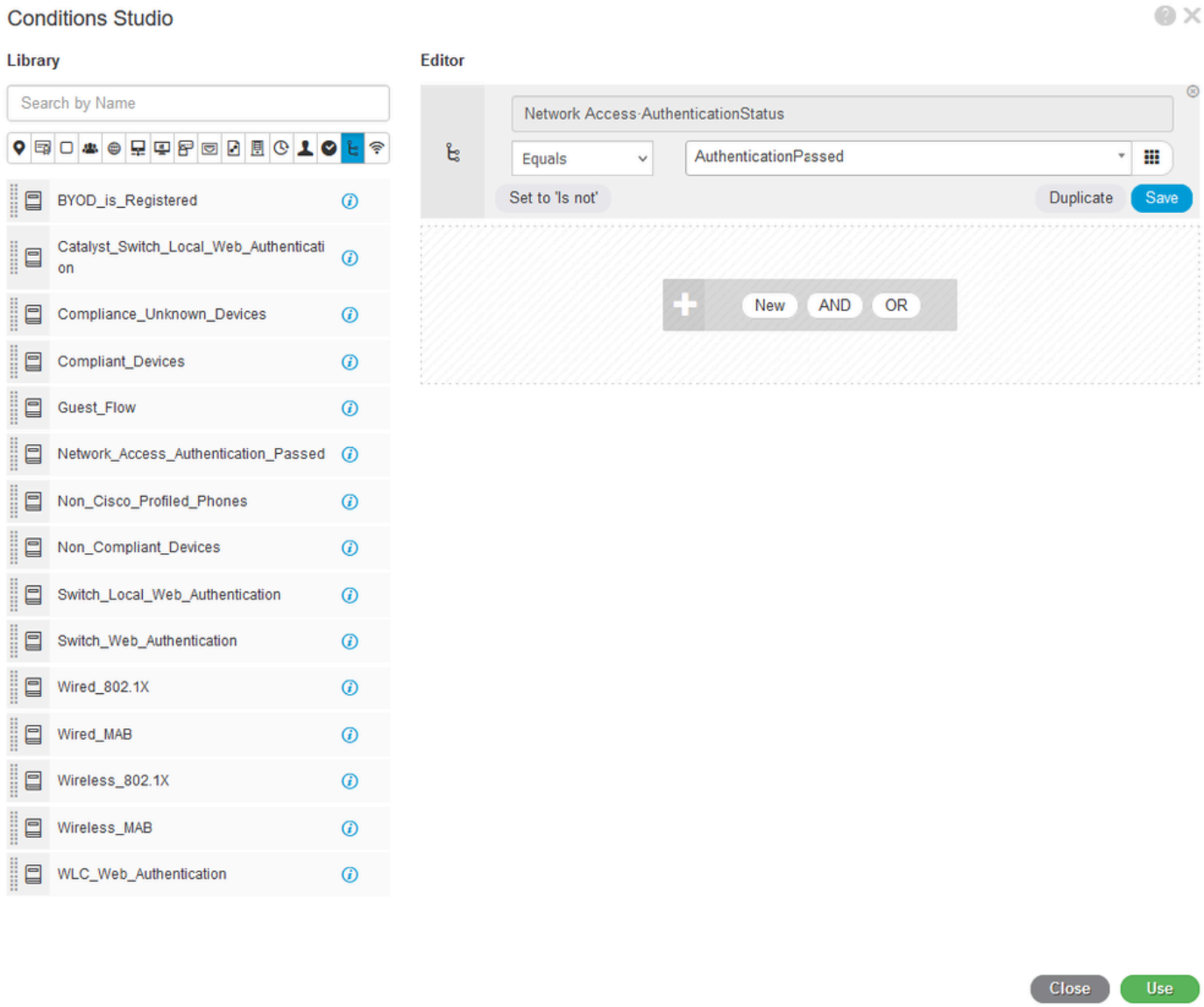
Nota: in questo esempio è consentita l'immissione dell'elenco Protocolli di accesso alla rete predefiniti. È possibile creare un nuovo elenco e restringerlo in base alle esigenze.

Passaggio 5. Per visualizzare i nuovi set di criteri, fare clic sull'icona ">" nella colonna Visualizza.

Passaggio 5.1. Espandere il menu Criteri di autorizzazione e fare clic sull'icona + per aggiungere una nuova regola che consenta l'accesso a tutti gli utenti autenticati.

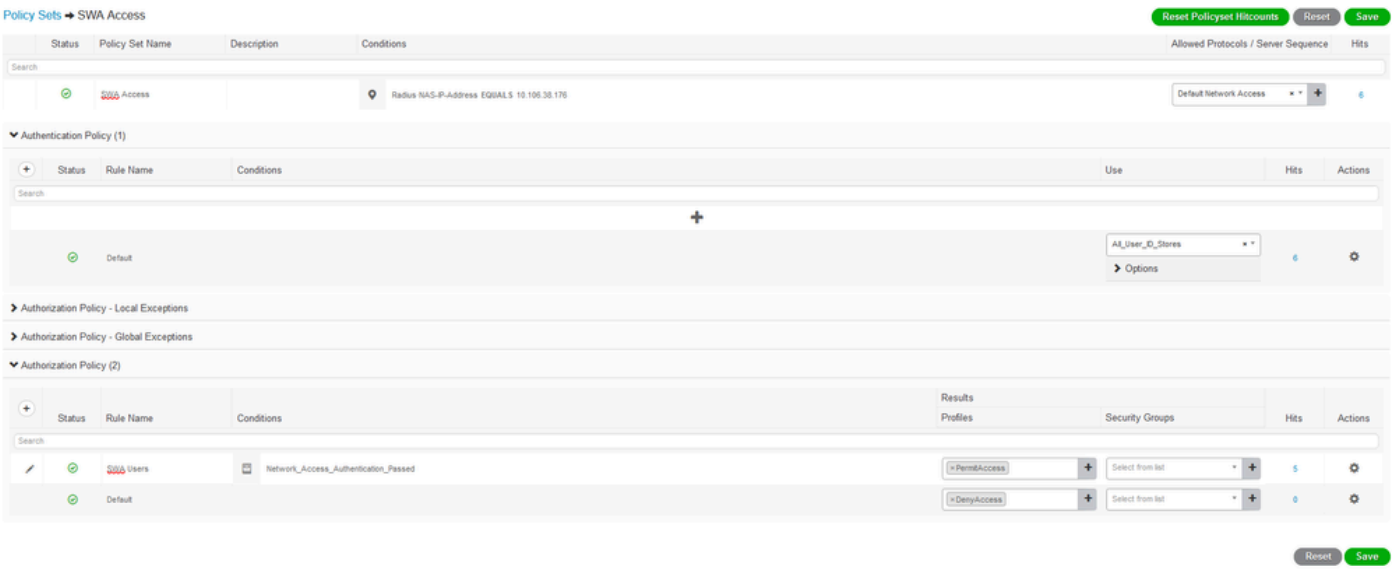
Passaggio 5.2. Impostare un nome.

Passaggio 5.3. Impostare le condizioni in modo che corrispondano all'accesso alla rete del dizionario con l'attributo AuthenticationStatus uguale a AuthenticationPassed e fare clic su Use.



Seleziona condizione di autorizzazione

Passaggio 6. Impostare il PermitAccess predefinito come profilo di autorizzazione e fare clic su Salva.

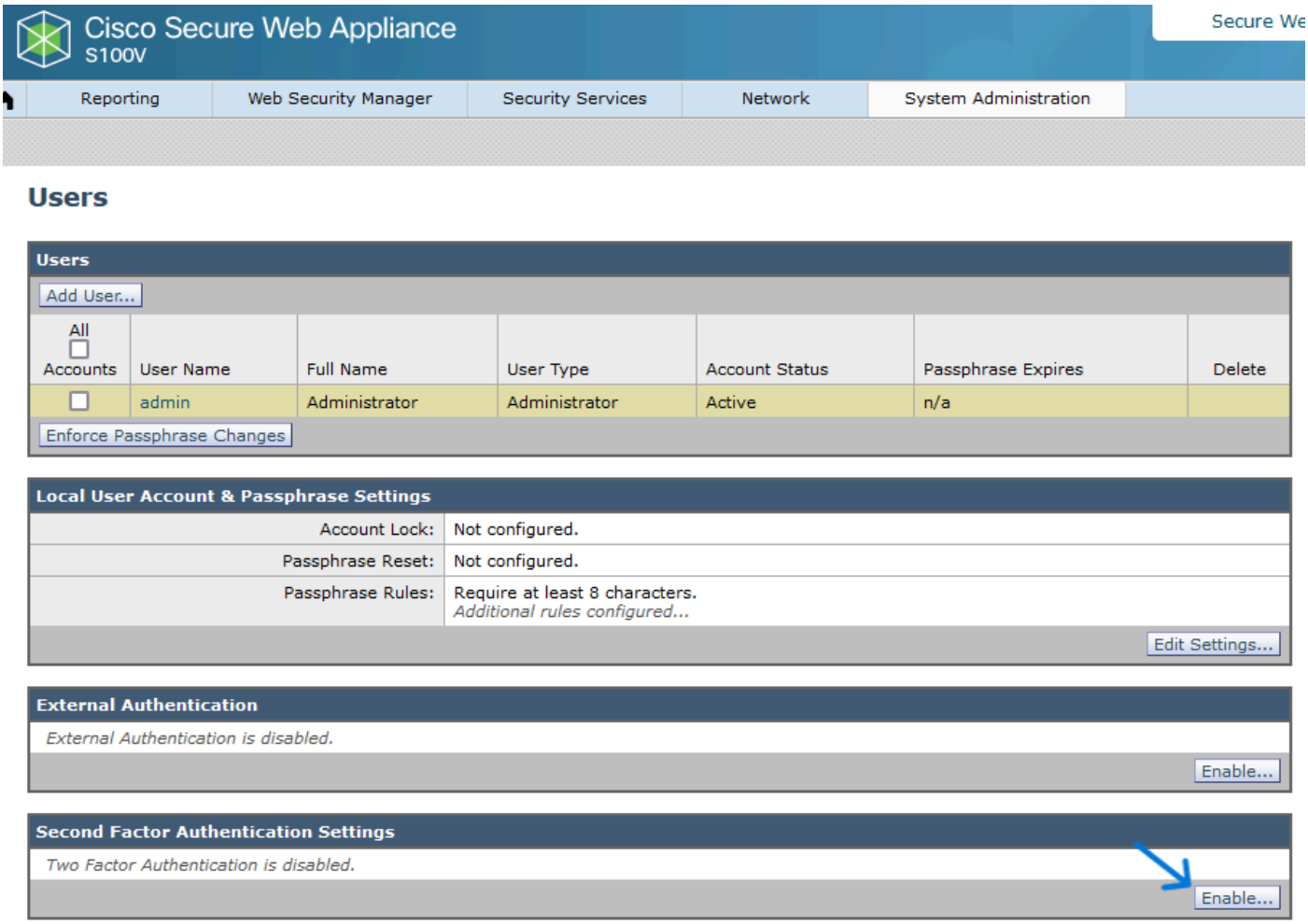


Seleziona profilo di autorizzazione

Configurazione SWA

Passaggio 1. Dalla GUI SWA, passare a System Administration (Amministrazione sistema) e fare clic su Users (Utenti).

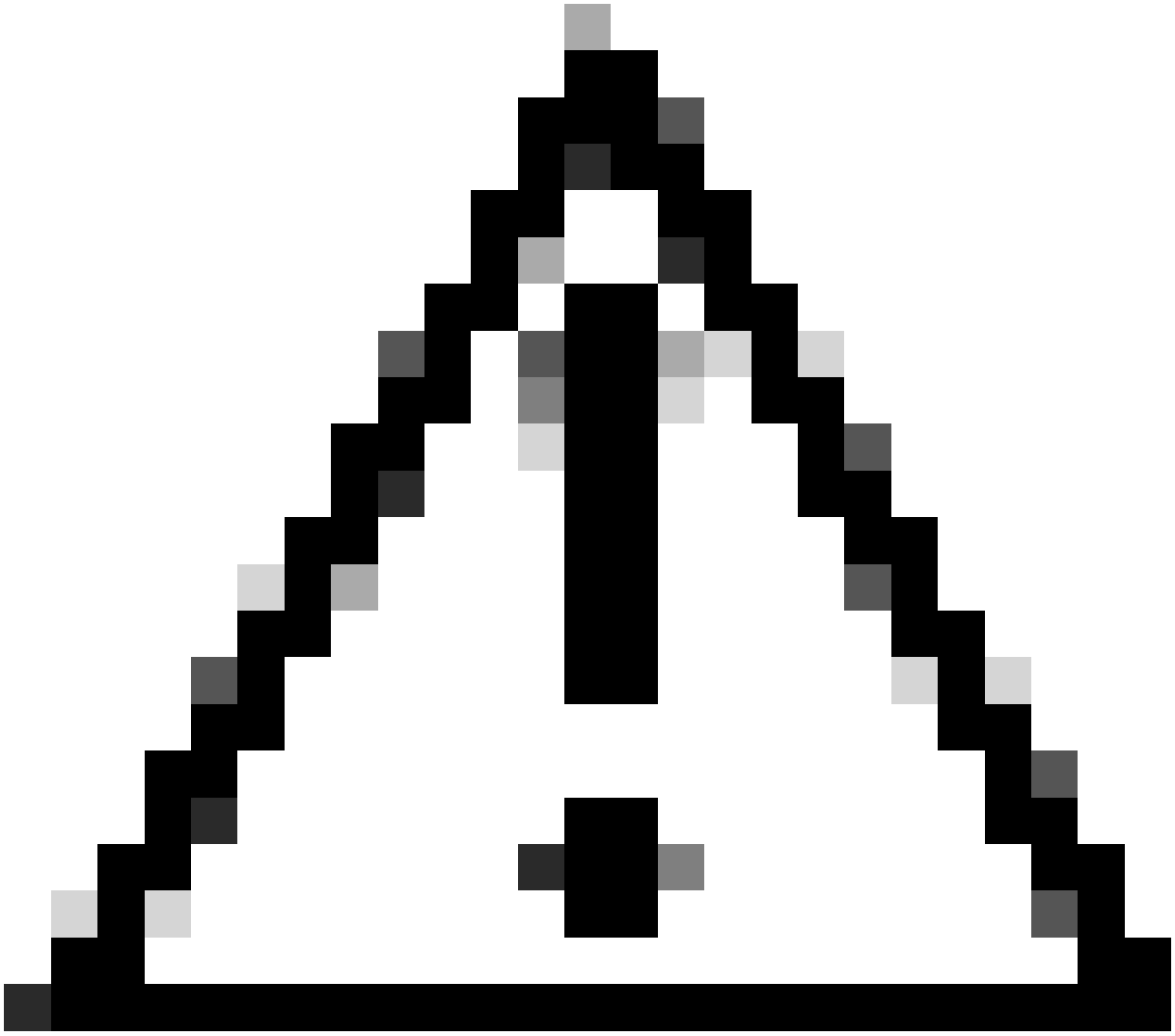
Passaggio 2. Fare clic su Enable (Abilita) in Second Factor Authentication Settings (Impostazioni seconda autenticazione).



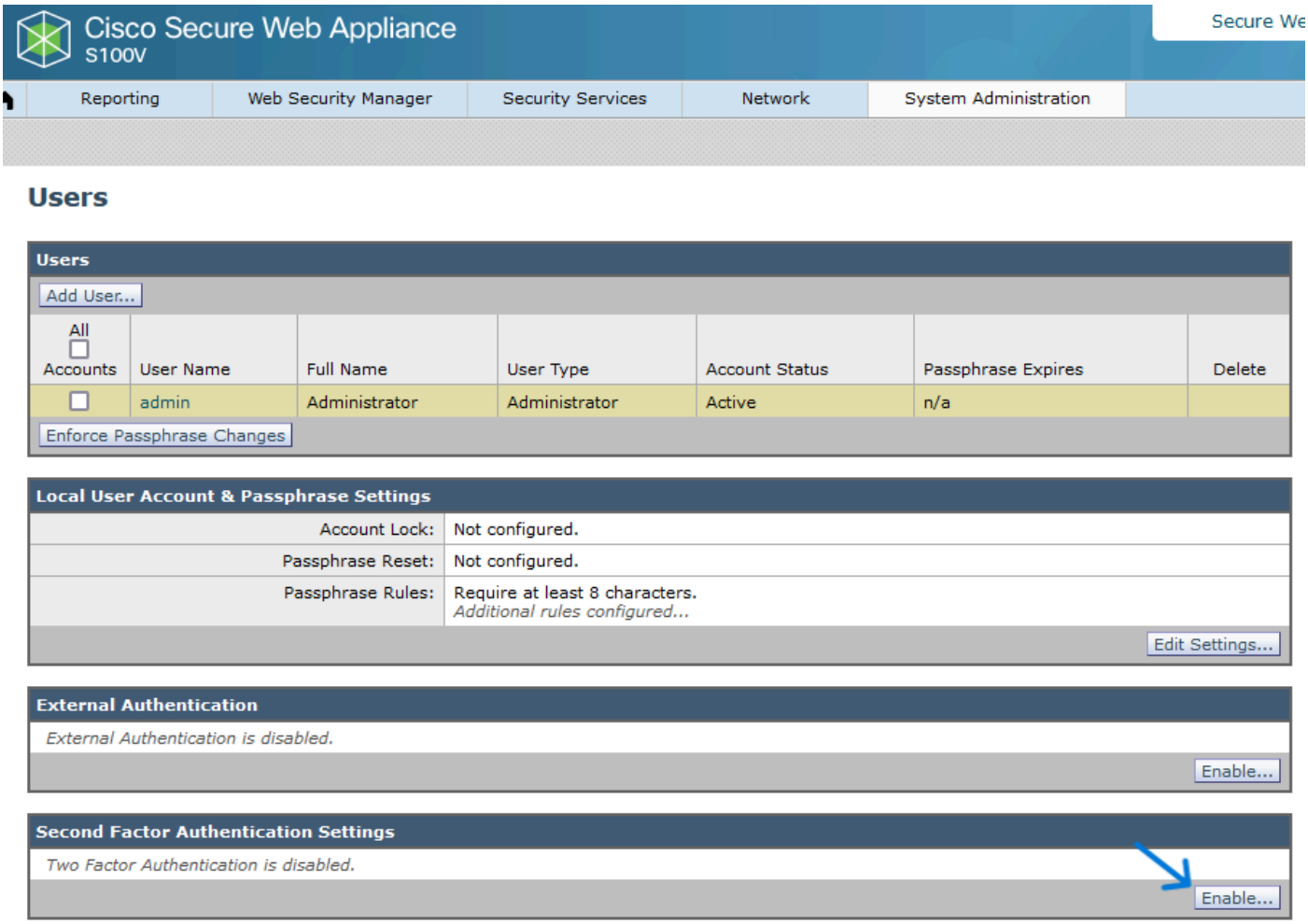
Abilitazione di Second Factor Authentication in SWA

Passaggio 3. Immettere l'indirizzo IP dell'ISE nel campo RADIUS Server Hostname e immettere il segreto condiviso configurato nel passaggio 2 della configurazione ISE.

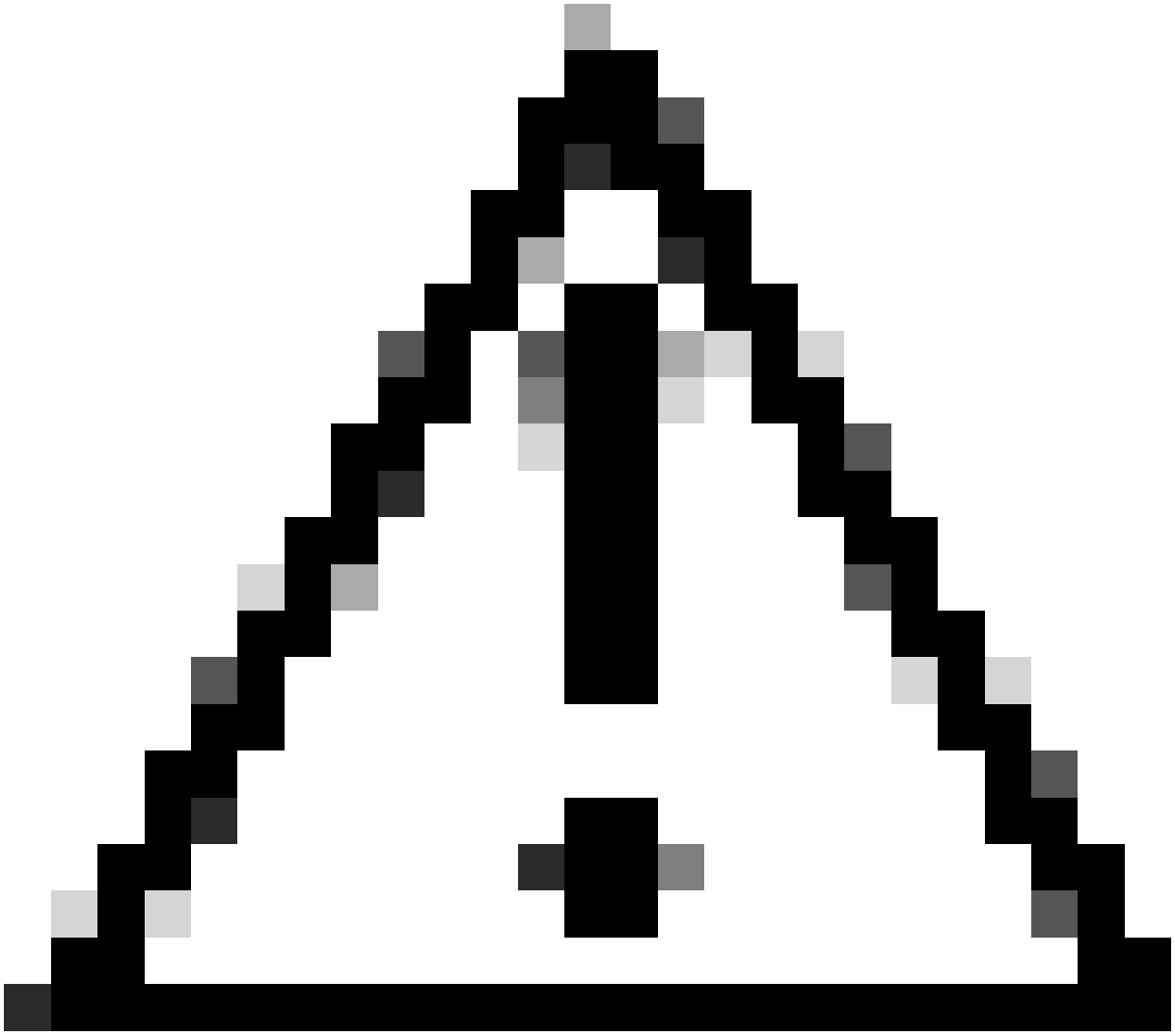
Passaggio 4. Selezionare i ruoli predefiniti obbligatori per i quali è necessario attivare l'applicazione di un secondo fattore.



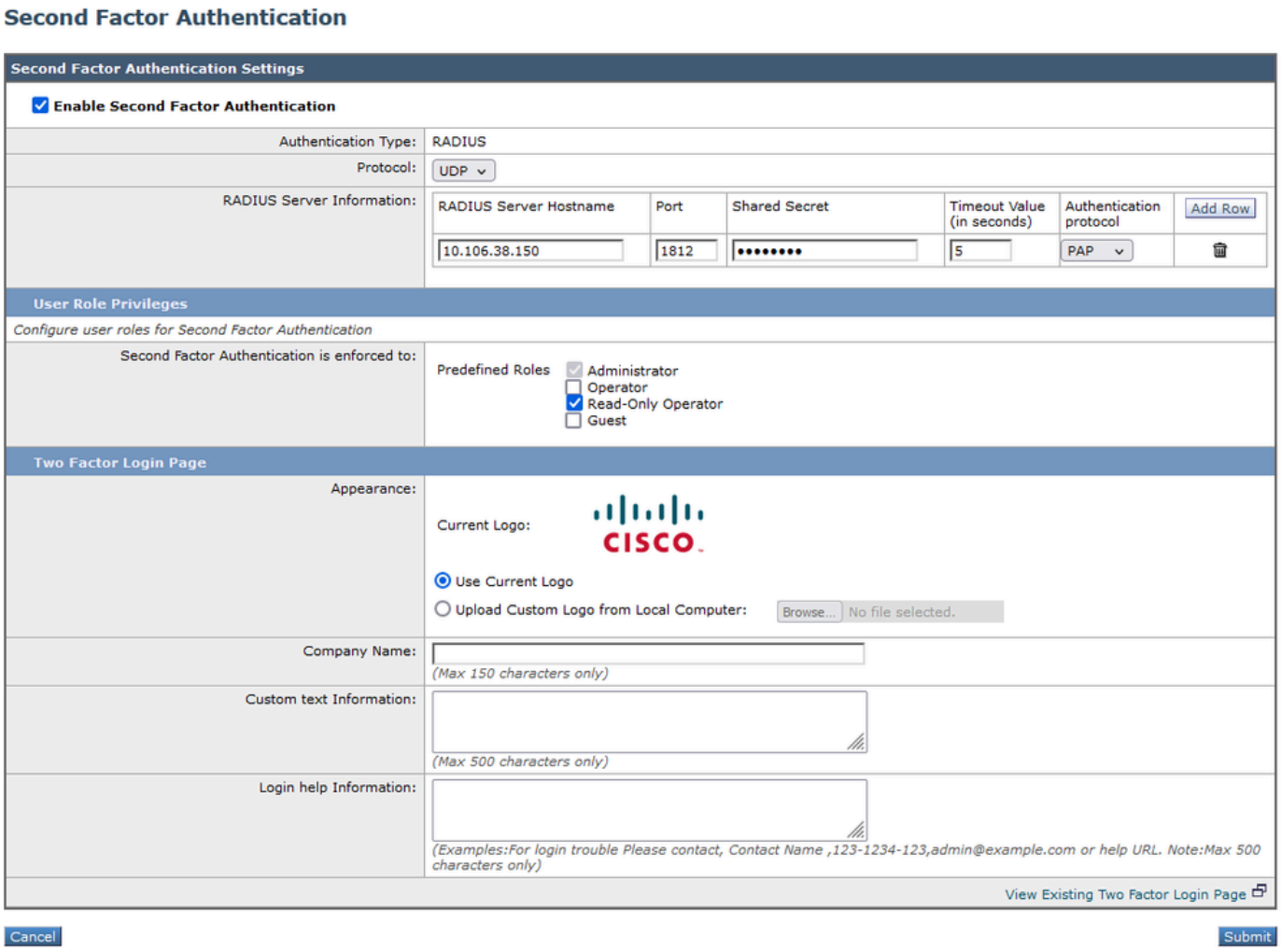
Attenzione: se si abilita l'autenticazione di secondo fattore in SWA, l'account predefinito 'admin' verrà abilitato anche con l'applicazione di secondo fattore. È necessario integrare ISE con LDAP o Active Directory (AD) per autenticare le credenziali 'admin', in quanto ISE non consente di configurare 'admin' come utente di accesso alla rete.



Abilitazione di Second Factor Authentication in SWA

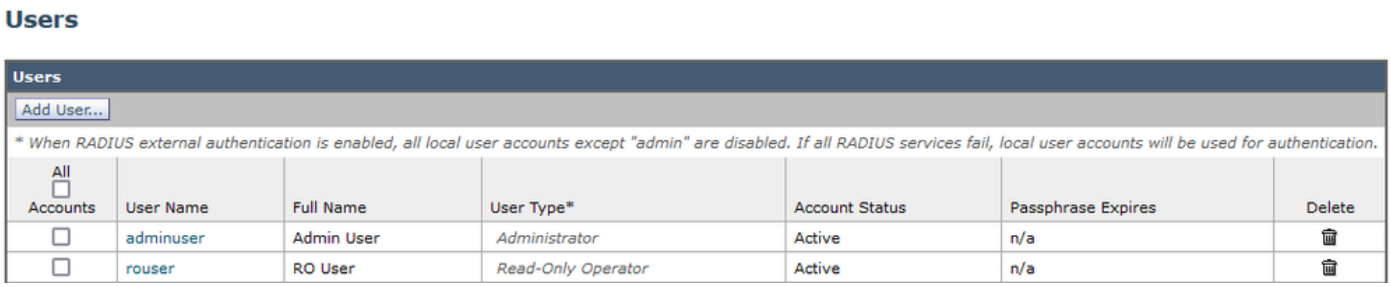


Attenzione: se si abilita l'autenticazione di secondo fattore in SWA, l'account predefinito 'admin' verrà abilitato anche con l'applicazione di secondo fattore. È necessario integrare ISE con LDAP o Active Directory (AD) per autenticare le credenziali 'admin', in quanto ISE non consente di configurare 'admin' come utente di accesso alla rete.



Configura autenticazione di secondo fattore

Passaggio 5: per configurare gli utenti in SWA, fare clic su Aggiungi utente. Immettere Nome utente e selezionare Tipo utente richiesto per il ruolo desiderato. Immettere Passphrase e Digitare nuovamente Passphrase.

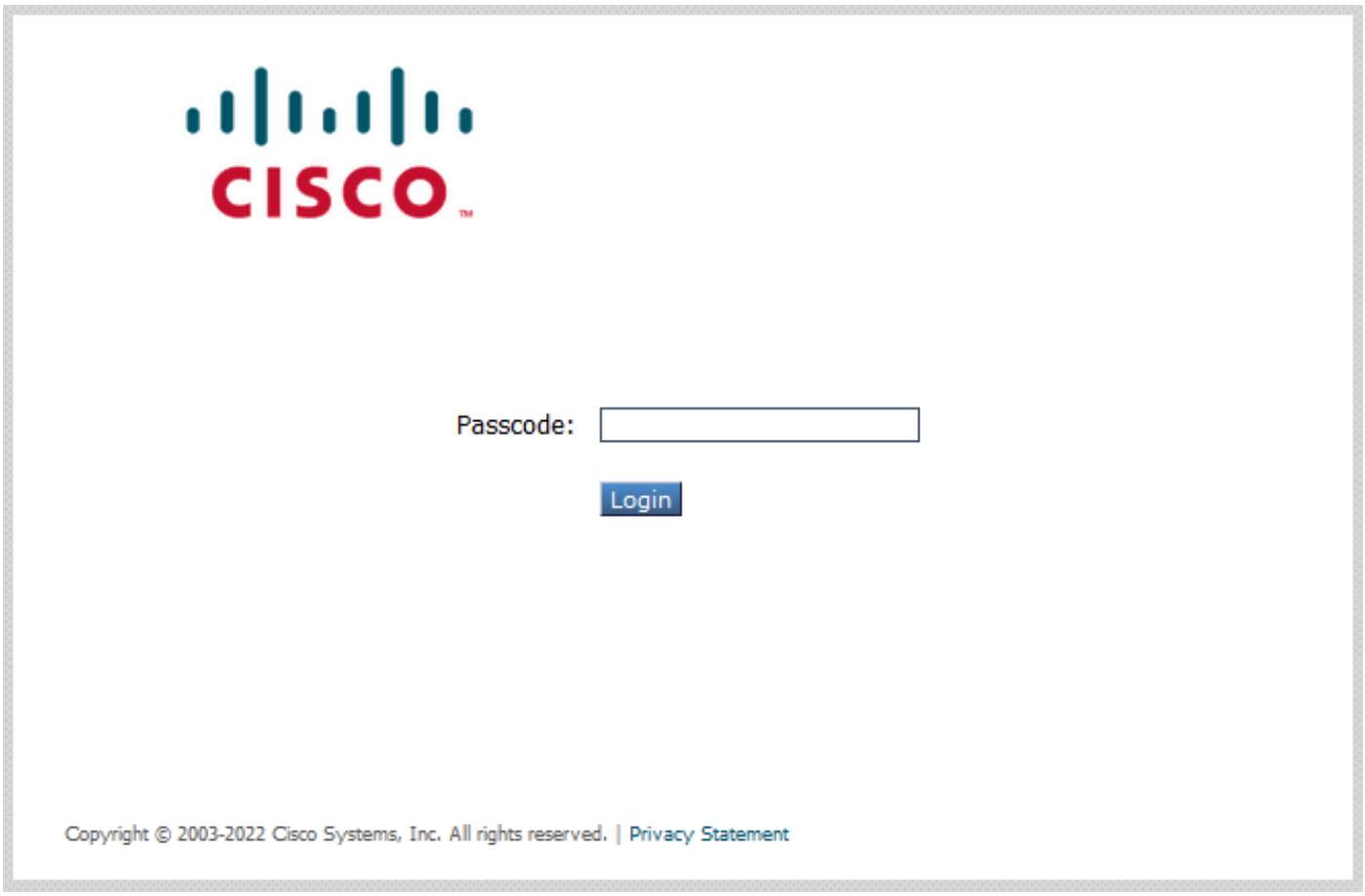


Configurazione utente in SWA

Passaggio 6: fare clic su Sottometti e conferma modifiche.

Verifica

Accedere all'interfaccia grafica SWA con le credenziali utente configurate. Una volta completata l'autenticazione, si viene reindirizzati alla pagina dell'autenticazione secondaria. Qui è necessario immettere le credenziali di autenticazione secondaria configurate in ISE.



Verifica accesso secondo fattore

Riferimenti

- Guida per l'utente di AsyncOS 14.0 per Cisco Secure Web Appliance
- Guida per l'amministratore di ISE 3.0
- ISE Compatibility Matrix per Secure Web Appliance
- Integrazione di AD per l'interfaccia grafica ISE e accesso tramite CLI

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).